REMARKS

Reconsideration of the subject application in view of the present amendments and remarks is respectfully requested. All rejections and objections are respectfully traversed.

Allowable Subject Matter

The Examiner has indicated that claims 7-9 and 16-18 would be allowable if rewritten in independent form including all limitations of the base claim and any intervening claims.

Applicant has amended claim 7 to incorporate the subject matter of independent claim 1, from which it depends. Applicant submits, therefore, that claims 7-9 and 16-18 are in condition for allowance and a notice to that effect is respectfully requested.

Claim Objections

The Examiner has objected to claims 2-18 due to informalities in the claims. Applicant has amended the claims to address the issue raised by the Examiner. Applicant submits that no new matter has been added. Applicant requests that the objections to claims 2-18 be withdrawn.

Rejections Under 35 U.S.C. §102

Claims 1-6 and 10-15 stand rejected under §102(b) as being anticipated by Cunningham et al., EP 0 986 229 (A2). Applicant respectfully traverses these rejections as set forth hereafter.

Generally, as described in the specification, embodiments of the present invention make it possible to monitor the dissemination of information by ensuring an effective interception of information that is sent from a network. (Spec, p. 1, lines 17-21). The reliable and fast identification of predetermined information enables the identification of documents being transmitted even when the quantity of information from a network is very large. (Spec, p. 1, lines 20-24). An interception system according to the present invention stops an attempt to disseminate documents if such a dissemination does not comply with the usage rights associated with those documents, for example, an emailed document sent to several addressees may be received by some but not others if the system has detected that the document should not be sent to such other addressees. (Spec, p. 19, line 30-p. 20, line 35).

Cunningham relates to a method and system for monitoring and controlling network access. More specifically, Cunningham aims at ensuring that the employees of an organization are appropriately managed according to the access control policies of that organization. (Col. 2, ¶ 7). In particular, access control policies are put in place in order to ensure that internet access is used primarily for business purposes and to maximize the internet connection capability. (Col. 2, ¶ 8). The access control is based on processing communication contractual information so as to check that the exchanges are in agreement with the rules defined by the organization. "One of the sets of rules relates to access management requirements for outgoing access, while the second set relates to inbound connection attempts." (Col. 10, ¶ 39). These rules may include information such as user names, authorized time periods and group names. (Col. 10, ¶¶ 40 and 41).

In contrast to Cunningham, claim 1 addresses the content of exchanged data so as to be able to prevent dissemination of otherwise sensitive information. Specifically, claim 1 recites, among other limitations, a system for intercepting multimedia documents from a first network and includes "means for creating an automaton for processing the received packet belonging to a new connection if the packet header analyzer means show that a packet under analysis constitutes a request for a new connection." Further, "a triplet comprising <identifier, connection state flag, storage container>" is created and "associated with each connection by said means for creating an automaton."

Cunningham does not take into account the nature of the exchanged data. Cunningham's access control ignores the content of any exchanged documents as such a system does not try to determine whether such documents, such as an image or financial information, includes sensitive elements, i.e., elements protected by confidentiality or copyright, for example.

The system according to the present invention is thus configured in such a manner that the automaton may be created "on the fly," in that the automaton is created, as recited in claim 1, "if the packet header analyzer means show that a packet under analysis constitutes a request for a new connection." This enables the system to simultaneously manage several connections with a possibility that the transfer of data is blocked for a specific connection whereas the transfer of that same data may continue without restriction for another connection.

Cunningham fails to disclose, teach or even suggest such specific features as recited in claim 1 and therefore cannot anticipate that which is recited in the claim.

As claims 10-15 depend, either directly or indirectly from claim 1, Applicant respectfully submits that these claims are also not anticipated by the Cunningham reference.

Claims 2 and 3, which depend from independent claim 1, recite "a first table for setting up a connection" and a "second table for identifying containers."

Applicant respectfully submits that Cunningham cannot anticipate claims 2 and 3 because Cunningham fails to disclosure a container dedicated to the storage of data extracted from a connection. Accordingly, for at least these reasons, claims 2 and 3 are also not anticipated by the Cunningham reference.

Claim 4, depends from claim 1 and further recites that the means recited in claim 1 "operate in an independent and asynchronous manner."

Applicant submits that Cunningham fails to disclose such a feature in those portions cited by the Examiner. Accordingly, Applicant respectfully submits that claim 4 is not anticipated by the Cunningham reference.

Claim 5 depends from claim 1 and further comprises a first module "for storing the content of documents intercepted by the module for intercepting and processing packets" and a second module "for storing information relating to at least the sender and the destination of intercepted documents." Thus, when intercepting an intention to send or download a web page or a file, the intention in question is stored pending interception of the page or file in question. (Spec, p. 20, lines 22-25).

Claim 6, which is dependent from claim 5, further recites a module "for storing information relating to the components that result from detecting the content of intercepted documents."

Cunningham does not analyze the content of transmitted documents and therefore also fails to disclose any module that would be analogous to the modules recited in claims 5 or 6. Accordingly, Applicant respectfully submits that claims 5 and 6 are not anticipated by the Cunningham reference.

New independent claim 19 incorporates the subject matter of independent claim 1 and claims 4 and 5. Thus, for at least the reasons submitted above with respect to claims 1, 4 and 5, Applicant respectfully submits that claim 19 is patentable over the Cunningham reference.

In view of the foregoing, Applicant believes the pending claims are in condition for allowance and a notice to this effect is earnestly solicited. The Examiner is encouraged to telephone the undersigned attorney to discuss any matter that would expedite allowance of the present application. The Examiner is hereby authorized to charge any fees due to this submission, or credit any balance, to Deposit Account No. 23-0804.

Respectfully submitted,

Hassane ESSAFI

Dated: May 10, 2010

By:/paul d sorkin/
Paul D. Sorkin, Reg. No. 39,039

WEINGARTEN, SCHURGIN,
GAGNEBIN & LEBOVICI LLP
Ten Post Office Square
Boston, MA 02109
Telephone: 617.542.2290 Fax: 617.451.0313

/